

A Note on the Injection Distance

Stanislav Bulygin*, Olav Geil† and Diego Ruano†

*Center for Advanced Security Research Darmstadt, Technische Universität Darmstadt, Germany

Email: Stanislav.Bulygin@cased.de

†Department of Mathematical Sciences, Aalborg University, Denmark

Email: {olav,diego}@math.aau.dk

Abstract—Kötter and Kschischang showed in [1] that the network coding counterpart of Gabidulin codes performs asymptotically optimal with respect to the subspace distance. Recently, Silva and Kschischang introduced in [2] the injection distance to give a detailed picture of what happens in noncoherent network coding. We show that the above codes are also asymptotically optimal with respect to this distance.

I. INTRODUCTION

The concept of error correction in linear network coding was introduced by Cai and Yeung in [3], [4] and [5]. The scenario considered there is known as coherent network coding meaning that the network topology as well as the linear network code are assumed to be known both to the sender and to the receivers.

Noncoherent network coding was considered by Kötter and Kschischang in [1] for the first time. Here, neither the sender nor the receivers are assumed to know the topology or the linear network code. To mimic the communication situation Kötter and Kschischang coined the concept of an operator channel which takes as input and output subsets of some fixed ambient vector space W . The set of vector subspaces is denoted by $\mathcal{P}(W)$. The game of error correction now is to identify the set of messages with a collection of subspaces $C \subseteq \mathcal{P}(W)$ called a subspace code. If C has been chosen cleverly it will, under certain assumptions, be possible to recover the message at the receiving end by performing some decoding algorithm. As part of their description they introduced the subspace distance in $\mathcal{P}(W)$. Using this distance then a minimum distance of C is obtained. Let t be the number of errors and ρ be the number of erasures occurred during the transmission over the channel (we will not formally define here what these concepts mean). The original message can be recovered if $2(t + \rho)$ is less than the minimum distance of the subspace code under consideration. However, the converse does not necessarily hold. Kötter and Kschischang adapted the rank-metric code construction by Gabidulin to work in the above setting and gave an efficient decoding algorithm for them. They presented a Singleton bound and demonstrated that the adapted Gabidulin codes attain it asymptotically.

In [2] Silva and Kschischang considered a slightly different model of non-coherent network coding. In particular they coined a new distance, namely the injection distance. Their interpretation of the number t of errors and the number ρ of erasures also differs from the one in [1]. The advantage of the model in [2] is that it allows not only a sufficient, but

also a necessary condition for decoding to be possible. We now describe the model in detail. As above each message is identified with a codeword in $C \subseteq \mathcal{P}(W)$. The sender injects a possibly overcomplete basis for this subspace into the network. The nodes then forward a linear combination of the incoming vectors on each outgoing edge and possibly add an error vector. Let X be an $n \times m$ matrix which rows are the source packets and for a specific receiver denote by Y the $N \times m$ matrix which rows are the received packets. Let the number of error vectors be t and denote by Z the $t \times m$ matrix which rows are the errors. With respect to the specific receiver let A be the $N \times n$ transfer matrix for the linear code (the error free part) and let D be the $N \times t$ transfer matrix for the errors. This gives us the model

$$Y = AX + DZ.$$

The transfer matrices A and D are unknown to the receiver and are chosen by the adversary while respecting the constraint $\text{rank}(A) \geq n - \rho$. Here, ρ is a parameter called the rank deficiency of A , known to all the participants. Knowing Y the decoding rule to use is

$$\hat{X} = \operatorname{argmin}_{X \in C} \Delta_\rho(X, Y)$$

where

$$\begin{aligned} & \Delta_\rho(X, Y) \\ &= \min\{r \mid A \in \mathbf{F}_q^{N \times n}, r \in \mathbf{N}, D \in \mathbf{F}_q^{N \times r}, \\ & \quad Z \in \mathbf{F}_q^{r \times m}, Y = AX + DZ, \text{rank}(A) \geq n - \rho\} \\ &= \max\{\dim(X) - \rho, \dim Y\} - \dim(X \cap Y). \end{aligned}$$

Here, the last equality corresponds to [2, Theorem 16]. The ability of a subspace code C to support the above decoding algorithm is described by the following parameter.

Definition 1: The injection distance between spaces $U, V \in \mathcal{P}(W)$ is defined as follows

$$d_I(U, V) = \dim(U + V) - \min\{\dim(U), \dim(V)\}.$$

This in an obvious way translates into a minimum distance $d(C)$ for any subspace code $C \subseteq \mathcal{P}(W)$.

Theorem 1: Assume there is a bijective map between the set of messages and the subspace code C . The code is guaranteed to correct t packet errors, under rank deficiency ρ , if and only if $d_I(C) > 2t + \rho$.

The injection distance relates to the subspace distance d_S from [1] as follows

$$d_I(U, V) = \frac{1}{2}d_S(U, V) + \frac{1}{2}|\dim(U) - \dim(V)|.$$

Hence, except for a factor $\frac{1}{2}$ the two distances are the same if $\dim(U) = \dim(V)$. A subspace code C is called equidimensional if all of its codewords have the same fixed dimension. It is clear that except for a factor $\frac{1}{2}$ the minimum distance of an equidimensional subspace code is the same no matter which of the metrics d_I or d_S is used.

II. ASYMPTOTIC RESULTS

A subspace code $C \subset \mathcal{P}(W)$ with W an N -dimensional vector space over \mathbb{F}_q (the finite field with q elements), with size $|C|$, maximum dimension of a codeword $l = \max_{x \in C} \dim(x)$ and minimum injection distance $D = d_I(C)$ is said to be of type $[N, l, \log_q |C|, D]$. The parameter

$$R = \frac{\log_q(|C|)}{Nl}$$

is called the rate of the code (see [1, Definition 2]). This parameter clearly serves as a measure of the efficiency of communication in a model where every block of information consists of l vectors of size N that are injected into the system. In other words, in a situation where we inject a possible overcomplete basis of l vectors into the system, the dimension of the codeword is unimportant. Following the ideas of [1] we will give a Singleton type upper bound on $|C|$ in terms of l, D and N . This will then give us an upper bound for R which we finally show to be reached asymptotically by the network coding counterparts of Gabidulin codes.

We consider the definition of puncturing from [1].

Definition 2: Let $C \subset \mathcal{P}(W)$, with $\dim(W) = N$ and let W' be a subspace of W of dimension $N - 1$. A punctured code C' is constructed from C by replacing $V \in C$ by $V' = \mathcal{H}_{\dim(V)-1}(V \cap W')$. That is,

- $V' = V \cap W'$, if $V \cap W'$ has dimension $\dim(V) - 1$.
- V' a random subspace of dimension $\dim(V) - 1$, otherwise.

We remark that the definition of C' is not unique.

This definition allows us to extend [1, Theorem 8] for the injection distance.

Proposition 1: Let C be a $[N, l, \log_q |C|, D]$ code with $d_I(C) = D > 1$. Then a punctured code C' is of type $[N - 1, l - 1, \log_q |C|, D']$, with $D' \geq D - 1$.

Proof: It is clear that $\dim W' = N - 1$ and the maximum dimension of the codewords is $l - 1$.

Let $U, V \in C$ with $U \neq V$, $l_1 = \dim(U)$ and $l_2 = \dim(V)$. Let $U' = \mathcal{H}_{l_1-1}(U)$ and $V' = \mathcal{H}_{l_2-1}(V)$. One has that $\dim(U \cap V) \leq \max\{l_1, l_2\} - D$ and therefore $\dim(U' \cap V') \leq \dim(U \cap V) \leq \max\{l_1, l_2\} - D$ since $U' \subset U$ and $V' \subset V$.

Hence,

$$\begin{aligned} d(U', V') &= \max\{l_1 - 1, l_2 - 1\} - \dim(U' \cap V') \\ &= \max\{l_1, l_2\} - 1 - \dim(U' \cap V') \\ &\geq D - 1 \end{aligned}$$

Since $D > 1$, we have as many codewords in C' as in C . \square

For nonnegative integers l, n with $l \leq n$, the q -ary Gaussian coefficient is

$$\begin{bmatrix} N \\ l \end{bmatrix}_q = \prod_{i=0}^{l-1} \frac{q^{N-i} - 1}{q^{l-i} - 1}$$

and for $l = 0$ is defined to be 1. The number of vector subspaces of dimension l of an N -dimensional vector space is given by $\begin{bmatrix} N \\ l \end{bmatrix}_q$. We may establish a Singleton type bound for codes with $l \leq N/2$ and the injection distance. This result extends [1, Theorem 9] where a Singleton bound is established for the subspace distance and equidimensional codes.

Theorem 2: Let C be a $[N, l, \log_q |C|, D]$ code, with $l \leq N/2$. Then,

$$|C| \leq 1 + (l - D + 1) \begin{bmatrix} N - D + 1 \\ N - l \end{bmatrix}_q.$$

Proof: We can puncture $D - 1$ times the code C to obtain a code C' of type $[N - (D - 1), l - (D - 1), \log_q |C|, D']$, with $D' \geq 1$, by Proposition 1 (if $D = 1$ we do not puncture it and $C = C'$). One has that $C' \subset W'$, with $\dim(W') = N - D + 1$. We bound the number of subspaces of W' with dimension lower than or equal to $l - D + 1$:

$$\begin{aligned} |\mathcal{P}(W', \leq l - D + 1)| &= \sum_{i=0}^{l-D+1} \begin{bmatrix} N - D + 1 \\ i \end{bmatrix}_q \\ &\leq 1 + (l - D + 1) \begin{bmatrix} N - D + 1 \\ l - D + 1 \end{bmatrix}_q \\ &= 1 + (l - D + 1) \begin{bmatrix} N - D + 1 \\ N - l \end{bmatrix}_q, \end{aligned}$$

$$\text{since } \begin{bmatrix} N \\ l \end{bmatrix}_q = \begin{bmatrix} N \\ n-l \end{bmatrix}_q.$$

For a code with $l > N/2$ a Singleton bound would be a trivial bound because, for N fixed, $\begin{bmatrix} N \\ l \end{bmatrix}_q$ is a symmetric function on l which has a maximum at $l = N/2$, for N even, or two maximums at $l = (N - 1)/2, (N + 1)/2$, for N odd.

Remark 1: In [1, Theorem 9], for equidimensional codes and the subspace distance, a Singleton bound is obtained by considering a punctured code and bounding the number of vector subspaces. The same argument is considered for the dual code, since $d_S(U, V) = d_S(U^\perp, V^\perp)$. The bound is the minimum of these two values.

Although for $U, V \in \mathcal{P}(W)$, $d_I(U, V) = d_I(U^\perp, V^\perp)$, one cannot consider the dual of C in the proof of the Singleton bound. Namely, let C be a code with dimension $l \leq N/2$ and let $l_1 < \dots < l_s = l$ the dimension of the words of C . One has that the words of C^\perp have dimension $N - l_s, \dots, N - l_1$,

and the words of its punctured code have dimension $N - l_s - D + 1, \dots, N - l_1 - D + 1$.

Let C be a code with $l = N/2 - 1$. Then the dimension of the smallest codeword of C^\perp is $l_1^\perp = N/2 + 1$. After puncturing it $D - 1$ times, one has that the dimension of the smallest codeword is $N/2 - D + 2$. Then,

$$|C'^\perp| \leq \sum_{i=0}^{N/2-1} \begin{bmatrix} N - (D-1) \\ N - i - (D-1) \end{bmatrix}_q,$$

however, it is not clear which of the Gaussian coefficients is the largest one. For instance, the largest Gaussian coefficient is $\begin{bmatrix} N-(D-1) \\ N-(N/2-1)-(D-1) \end{bmatrix}$ (for $(N/2 - D + 2)$ even) if and only if $N/2 - (D-1)/2 < N/2 + 2 - D$, that is, $D < 5$.

We consider the codes from [1, Section V-B], these codes are the translation of the Gabidulin rank-matrix code construction to subspace codes, these codes nearly achieve the Singleton bound for the subspace distance. Moreover, they verify the assumption $l \leq N/2$ and we claim that they also nearly achieve the Singleton-Bound for the injection distance (Theorem 2).

Gabidulin codes are equidimensional which allows us to calculate their injection distance as follows $d_I(C) = d_S(C)/2 = l - k + 1$. Here, the last part is from [1]. They are of type $[l+m, l, mk, l-k+1]$, with $l \leq m$ and $l \geq k$. We have that $l \leq N/2$, since $l \leq N/2$ if and only if $l \leq (l+m)/2$, that is, $l \leq m$.

We consider the bound from theorem 2,

$$\begin{aligned} |C| &\leq 1 + (l - (l - k + 1) + 1) \begin{bmatrix} N - ((l - k + 1) - 1) \\ N - l \end{bmatrix}_q \\ &= 1 + k \begin{bmatrix} l + m - l + k \\ l + m - l \end{bmatrix}_q \\ &= 1 + k \begin{bmatrix} m + k \\ m \end{bmatrix}_q \quad (1) \\ &< 1 + 4kq^{mk}. \quad (2) \end{aligned}$$

The last inequality follows from $1 < q^{l(N-l)} \begin{bmatrix} N \\ l \end{bmatrix}_q < 4$ (see [1, Lemma 4]).

Therefore, a code achieving the bound in Theorem 2 cannot have more than $4k$ times as many codewords as a Gabidulin code. Consider now the rate corresponding to (2)

$$R = \log_q(|C|)/Nl = \frac{\log_q(\frac{1}{q^{mk}} + 4k) + km}{Nl}.$$

As by construction $k \leq l$ this tends to $\frac{km}{Nl}$ as N goes to infinity. In other words the network coding counterpart of Gabidulin codes asymptotically has the maximal rate. The next example illustrates that already for small N the Gabidulin codes perform quite well.

Example 1: In this Example we consider codes of the Gabidulin type over the field \mathbb{F}_{16} , the finite field with 16 elements. We consider a sequence of values

$$\{[m_4, l_4, k_4], [m_5, l_5, k_5], \dots, [m_{30}, l_{30}, k_{30}]\}$$

with $m_i = i$, $l_i = \lfloor \frac{3m_i}{5} \rfloor$ and $k_i = \lfloor \frac{m_i}{2} \rfloor$ for $i = 4, \dots, 30$. The corresponding codes have length N equal to

$$\{6, 8, 9, \dots, 48\}.$$

In Figure 1, the rates of the Gabidulin type codes are plotted with \diamond 's. The '+'s correspond to the upper bound (1) and the 'o's correspond to the upper bound (2).

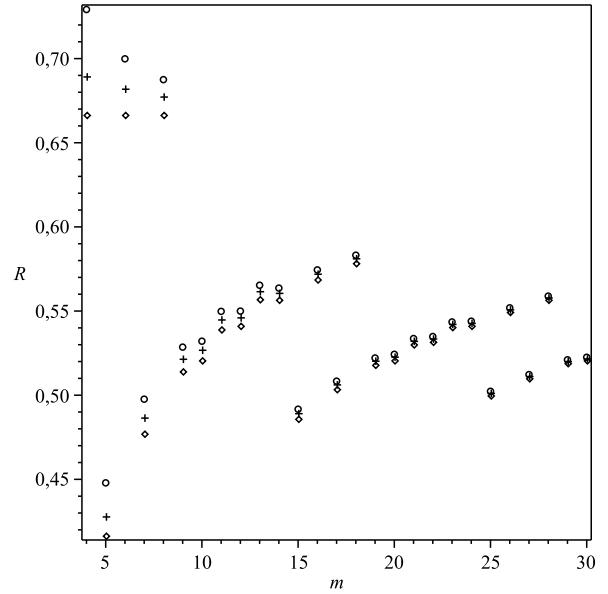


Fig. 1.

REFERENCES

- [1] R. Kötter and F. R. Kschischang, "Coding for Errors and Erasures in Random Network Coding," *IEEE Trans. Inform. Theory*, **54**(8), 2008, pp. 3579-3591.
- [2] D. Silva and F. R. Kschischang, "On Metrics for Error Correction in Network Coding," *ArXiv:0805.3824v4[cs.IT]*, 2009, To appear in *IEEE Trans. Inform. Theory*, 28 pages.
- [3] N. Cai and R. W. Yeung, "Network coding and error correction," in *Proc. 2002, IEEE Inform. Theory Workshop*, Oct. 20-25, 2002, pp. 119-122.
- [4] R. W. Yeung and N. Cai, "Network error correction, part I: Basic concepts and upper bounds," *Commun. Inform. Syst.*, **6**, No. 1, 2006, pp. 19-36.
- [5] N. Cai and R. W. Yeung, "Network error correction, part II: Lower bounds," *Commun. Inform. Syst.*, **6**, No. 1, 2006, pp. 37-54.